

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS**

BRANDON STRONG, on behalf of himself
and others similarly situated,

Plaintiff,

v.

**WEBTPA EMPLOYER
SERVICES, LLC,**

Defendant.

Case No. 3:24-cv-01343

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Brandon Strong, individually and on behalf of the Classes defined below of similarly situated persons (“Plaintiff and Class Members”), alleges the following against Defendant WebTPA Employer Services, LLC, (“Defendant”). The following allegations are based on Plaintiff’s knowledge, investigations by Plaintiff’s counsel, facts of public record, and information and belief:

NATURE OF THE ACTION

1. Plaintiff seeks to hold Defendant responsible for the injuries WebTPA inflicted on Plaintiff and over 2.4 million others due to Defendant’s egregiously inadequate data security, which resulted in the private information of Plaintiff and those similarly situated to be exposed to unauthorized third parties (the “Data Breach”).

2. WebTPA is a third-party administrator that creates custom health plans for employers that are made to lower health plan costs while providing competitive benefits. WebTPA also offers administrative services.

3. The data that WebTPA exposed to the public is unique and highly sensitive. For one, the exposed data included personal identifying information (“PII”) and protected health information (“PHI”) like name, contact information, date of birth, date of death, Social Security number, and insurance information, which Plaintiff and Class Members provided with the understanding WebTPA would keep that information private in accordance with both state and federal laws.

4. According to WebTPA, on December 28, 2023, WebTPA detected unusual activity on its internal computer network. WebTPA was able to determine that security and privacy of Plaintiff’s and Class Members’ PII and PHI was impacted between April 18, 2023 and April 23, 2023.

5. Among myriad industry standards and statutes for protection of sensitive information, PHI is specifically governed by federal law under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and its implementing regulations. HIPAA requires entities like WebTPA to take appropriate technical, physical, and administrative safeguards to secure the privacy of PHI, establishes national standards to protect PHI, and requires timely notice of a breach of unencrypted PHI.

6. Instead of following these rules, however, WebTPA disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement reasonable measures to safeguard Private Information and by failing to take necessary steps to prevent unauthorized disclosure of that information. WebTPA’s woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence.

7. Exacerbating the injuries to Plaintiff and Class Members, WebTPA failed to provide timely notice to Plaintiff and Class Members, depriving them of the chance to take speedy measures to protect themselves and mitigate harm. When WebTPA finally did notify Plaintiff and Class Members of the disclosure, WebTPA offered no assurances that all personal data or copies of data have been recovered or destroyed, or that WebTPA has adequately enhanced its security practices or dedicated sufficient resources and staff to avoid a breach of its network in the future..

8. Today, the PII and PHI of Plaintiff and Class Members continue to be in jeopardy because of Defendant's actions and inactions described herein. Plaintiff and Class Members now suffer from a heightened and imminent risk of fraud and identity theft for years to come and now must constantly monitor their medical and financial accounts for unauthorized activity.

9. The PII and PHI (collectively "Private Information") exposed in the Data Breach can enable criminals to commit a litany of crimes. Criminals can open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' health information to craft phishing and other hacking attacks based on Class Members' individual health needs, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

10. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have suffered actual and present injuries, including but not limited to: (a) present, certainly impending, and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of benefit of the bargain (price premium damages); (d) loss of value of privacy and confidentiality of the stolen

Private Information; (e) illegal sales of the compromised Private Information; (f) mitigation expenses and time spent responding to and remedying the effects of the Data Breach; (g) identity theft insurance costs; (h) “out of pocket” costs incurred due to actual identity theft; (i) credit freezes/unfreezes; (j) anxiety, annoyance, and nuisance; (k) continued risk to their Private Information, which remains in WebTPA’s possession and is subject to further breaches so long as WebTPA fails to undertake appropriate and adequate measures to protect Plaintiff’s and Class Members’ Private Information; and (l) disgorgement damages associated with WebTPA’s maintenance and use of Plaintiff’s data for its benefit and profit.

11. Through this action, Plaintiff seeks to remedy these injuries on behalf of himself and all similarly situated individuals whose Private Information was exposed and compromised in the Data Breach.

12. Plaintiff brings this action against WebTPA and assert claims for both damages and injunctive relief.

PARTIES

13. Plaintiff Brandon Strong is a natural person, resident, and citizen of Montana.

14. Defendant WebTPA is a limited liability company with its principal place of business and headquarters at 8500 Freeport Parkway South, Suite 400, Irving, Texas 75063.

JURISDICTION AND VENUE

15. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds \$5,000,000, exclusive of interest and costs. And minimal diversity is established because Plaintiff (and many members of the Nationwide Class) are citizens of states different than Defendant.

16. This Court has general personal jurisdiction over Defendant because Defendant's principal place of business and headquarters are in Irving, Texas. Defendant also regularly conduct substantial business in Texas.

17. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

FACTUAL ALLEGATIONS

Defendant Collected and Stored the Private Information of Plaintiff and Class Members

18. WebTPA is a third-party administrator that builds custom health plans for employers and provides administrative services.¹

19. Plaintiff and Class Members provided their Private Information to their respective benefit plans and insurance companies, those of which provided the Private Information to WebTPA to use WebTPA's administrative services.

20. WebTPA collects Private Information from Plaintiff and Class Members such as their names, contact information, birth dates, death dates, Social Security numbers, and insurance information in the ordinary course of business. Upon information and belief, this Private Information is then stored on Defendant's computer network.

21. Because of the highly sensitive and personal nature of the information WebTPA acquires and stores, WebTPA knew or reasonably should have known that it must comply with healthcare industry standards related to data security and all federal and state laws protecting Private Information and provide adequate notice if Private Information is disclosed without proper authorization.

¹ WebTPA Launch Site, WebTPA, <https://www.webtpa.com/> (last accessed May 14, 2024).

22. Indeed, WebTPA both explicitly and implicitly promised Plaintiff and Class Members that it used reasonable measures to safeguard the Private Information it collects from theft and misuse.

23. Recognizing its legal and equitable duties, WebTPA represents the following in its Privacy Statement:

WebTPA is committed to protecting your privacy and the confidentiality of your personal information. Personal information is any information that directly identifies or reasonably can be used to identify you.²

24. WebTPA misrepresented to Plaintiff and Class Members via its Privacy Statement that it implemented adequate technical measures to protect Plaintiff's and Class Members' Private Information:

How is your personal information protected?

WebTPA has implemented physical, electronic and technical safeguards to protect your personal information, consistent with applicable privacy and data security laws. However, we cannot completely guarantee security of your personal information.³

25. Upon information and belief, including from information gathered from the Data Breach at issue and subsequent cybersecurity issues within Defendant's computer network, that representation is not true.

26. Plaintiff and Class Members provided their Private Information to WebTPA as a condition of receiving administrative services from WebTPA, but in doing so, expected WebTPA to keep their Private Information confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

The Data Breach

² *WebTPA Privacy Statement*, WebTPA (Dec. 1, 2020), <https://www.webtpa.com/privacy>

³ *Id.*

27. The Notice of Data Breach posted by WebTPA on its website states:

WebTPA Employer Services, LLC (“WebTPA”) recently detected a data security incident impacting certain systems on our network. WebTPA acts as an administrative services provider to certain benefit plans and insurance companies whose information was impacted in this incident.

On December 28, 2023, we detected evidence of suspicious activity on the WebTPA network that prompted us to launch an investigation. Upon detecting the incident, we promptly initiated measures to mitigate the threat and further secure our network. We also launched an investigation with the support of industry leading third-party cybersecurity experts and notified federal law enforcement. The investigation concluded that the unauthorized actor may have obtained personal information between April 18 and April 23, 2023. WebTPA promptly informed benefit plans and insurance companies about the incident and the potential exposure of personal information. WebTPA then diligently worked to confirm the extent of impacted data, which we provided to benefit plans and insurance companies on March 25, 2024.

The information that was impacted may have included name, contact information, date of birth, date of death, Social Security number, and insurance information. Not every data element was present for every individual.

WebTPA is offering individuals two years of complimentary identity monitoring services through Kroll. We also deployed additional security measures and tools with the guidance of third-party cybersecurity experts to further strengthen the security of our network.

WebTPA is not aware of any misuse of benefit plan member information as a result of this incident. Financial information, such as financial account information or credit card numbers, and treatment or diagnostic information were not impacted.⁴

28. On May 8, 2024, WebTPA reported the Data Breach to the California Attorney General’s Office and included a sample data breach notification letter sent out to affected individuals, such as Plaintiff and Class Members. The sample data breach notification letter contains information about the Data Breach similar to what WebTPA posted on its website.⁵

⁴ *Notice of Data Security Incident*, WebTPA, <https://www.webtpa.com/notice> (last accessed May 14, 2024).

⁵ *Search Data Security Breaches*, Off. of the Cal. Atty Gen. (May 8, 2024), <https://oag.ca.gov/privacy/databreach/list>.

29. Upon information and belief, Plaintiff's and Class Members' affected Private Information at the time of the Data Breach was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals.

30. The Private Information of over 2.4 million individuals—including Plaintiff and Class Members—was compromised in the Data Breach.⁶

31. Upon information and belief, WebTPA was a target by due to its status as healthcare-related entity that collects, creates, and maintains Private Information.

32. The Notice of Data Breach gives no details to Plaintiff or Class Members regarding the manner and means of how their Private Information was disclosed and leaves Plaintiff and Class Members wondering how they can protect themselves.

33. Time is of the essence when highly sensitive Private Information is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired Private Information of Plaintiff and Class Members is now likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted Private Information to criminals.

34. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their Private Information, especially their Social Security numbers and sensitive medical information, onto the Dark Web. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing hundreds of thousands of Social Security numbers and/or specific, sensitive medical information.

⁶ *Breach Portal*, Dep't of Health and Hum. Servs. Off. for Civ. Rights (May 8, 2024), https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

35. WebTPA largely put the burden on Plaintiff and Class Members to take measures to protect themselves from identity theft and fraud.

36. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.6% of U.S.-based workers are compensated on an hourly basis, while the other 44.4% are salaried.⁷

37. According to the American Time Use Survey, American adults have between 4 to 6 hours of “leisure time” outside of work per day;⁸ examples of leisure time include partaking in sports, exercise and recreation; socializing and communicating; watching TV; reading; thinking/relaxing; playing games and computer use for leisure; and other leisure activities.⁹ Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

38. Plaintiff and Class Members are deprived of the choice as to how to spend their valuable free hours and therefore seek renumeration for the loss of valuable time as another element of damages.

⁷ *Characteristics of minimum wage workers, 2022*, U.S. Bureau of Labor Statistics (Aug. 2023), <https://www.bls.gov/opub/reports/minimum-wage/2022/home.htm#:~:text=The%20following%20are%20highlights%20from,federal%20minimum%20wage%20or%20less.>

⁸ *Americans have no idea how to use their free time*, Business Insider (Mar. 26, 2024), <https://www.businessinsider.com/americans-free-time-leisure-dont-use-television-2024-3#:~:text=Americans%20on%20average%2C%20have%20between,people%20spend%20doing%20various%20activities.>

⁹ *Table 11A. Time spent in leisure and sports activities for the civilian population by selected characteristics, averages per day, 2022 annual averages*, U.S. Bureau of Labor Statistics (June 22, 2023), <https://www.bls.gov/news.release/atus.t11A.htm>.

39. Defendant offered identity monitoring services for a period of two years. Such measures, however, are insufficient to protect Plaintiff and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide to Plaintiff and Class Members identity theft protection services for their respective lifetimes.

40. Plaintiff and the Class Members remain in the dark regarding exactly what data was stolen, the particular method of disclosure, the results of any investigations, and what steps are being taken, if any, to secure their Private Information going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

41. WebTPA could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' Private Information.

42. Defendant's negligence in safeguarding Plaintiff's and Class Members' PII and PHI was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

43. Healthcare organizations have become a main target for cybercriminals because they "hold a massive amount of patient data — including medical records, financial information, Social Security numbers, names and addresses. They're also among the few businesses that stay open 24/7, meaning they might be more likely to prioritize avoiding disruptions and, therefore, more likely to pay a hacker's ransom."¹⁰

¹⁰ Elise Takahama, *Why health care has become a top target for cybercriminals*, The Seattle Times (Feb. 25, 2024), <https://www.seattletimes.com/seattle-news/health/why-health-care-has-become-a-top-target-for-cybercriminals/>.

44. In the context of data breaches, healthcare is “by far the most affected industry sector.”¹¹ Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.¹²

45. Despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff’s and Class Members’ Private Information from being compromised.

46. WebTPA failed to properly train its employees as to cybersecurity best practices and to maintain proper staffing and processes for responding to and preventing network intrusions.

47. WebTPA failed to implement sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.

48. WebTPA failed to encrypt Plaintiff’s and Class Members’ Private Information and monitor user behavior and activity to identify possible threats.

49. WebTPA failed to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

50. WebTPA failed to timely and accurately disclose that Plaintiff’s and Class Members’ PII and PHI had been improperly acquired or accessed.

51. WebTPA knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII and PHI.

Defendant Failed to Comply with FTC Guidelines

¹¹ Tenable Security Response Team, *Healthcare Sec.*, TENABLE (Mar. 10, 2021), <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches>.

¹² See *id.*

52. According to the Federal Trade Commission (“FTC”), the need for data security should be factored into all business decision-making.¹³ To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII and PHI.

53. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.¹⁴ The guidelines explain that businesses should:

- a. protect the personal customer information that they keep;
- b. properly dispose of personal information that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network’s vulnerabilities; and
- e. implement policies to correct security problems.

54. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

55. The FTC recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.¹⁵

¹³ *Start with Security: A Guide for Business*, FED. TRADE COMM’N (Aug. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf.

¹⁴ *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM’N (Oct. 2016), <https://bit.ly/3u9mzre>.

¹⁵ *Start with Security: A Guide for Business*, FED. TRADE COMM’N (Aug. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf.

56. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”).

58. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

59. Despite its alleged commitments to securing sensitive data, WebTPA does not follow industry standard practices in securing Private Information.

60. As shown above, experts studying cyber security routinely identify healthcare related entities as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

61. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to, educating all employees on the risks of cyber attacks; strong passwords; multi-layer security, including

firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

62. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

63. Upon information and belief, WebTPA failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

64. Such frameworks are the existing and applicable industry standards in the healthcare industry. And WebTPA failed to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

Defendant Violated HIPAA and HITECH

65. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep medical information safe. HIPAA compliance provisions, commonly known as

the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.¹⁶

66. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.¹⁷

67. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

- a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);
- b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- d. Failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

¹⁶ HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

¹⁷ See 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

- e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);
- g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);
- h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and
- i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

68. Defendant WebTPA is a business associate under HIPAA and therefore must comply with HIPAA.¹⁸ The Data Breach, however, which resulted from a combination of insufficiencies, demonstrates that Defendant indeed failed to comply with safeguards mandated by HIPAA regulations.

¹⁸ Breach Portal, Dep’t of Health and Hum. Servs. Off. for Civ. Rights (May 8, 2024), https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

69. WebTPA is also required to follow the regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act (“HITECH”). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

70. Both HIPAA and HITECH obligate WebTPA to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive Private Information. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); 45 C.F.R. § 164.530(f); 42 U.S.C. § 17902.

Plaintiff’s Experiences and Injuries Caused by the Data Breach

71. Plaintiff and Class Members are current and former patients/customers of benefits plans and insurance companies which used WebTPA’s administration services.

72. As a prerequisite of receiving administrative services from WebTPA, Defendant required Plaintiff and Class Members to provide their Private Information.

73. WebTPA began notifying Plaintiff and Class Members about the Data Breach on or around April 11, 2024.

74. When WebTPA finally announced the Data Breach, it deliberately underplayed the severity and obfuscated the nature of the Data Breach. Defendant’s Notice of Data Breach and breach notification letter fail to adequately explain how the breach occurred, what exact data elements of each affected individual were compromised, and the extent to which those data elements were compromised.

75. Because of the Data Breach, Defendant inflicted injuries upon Plaintiff and Class Members. And yet, Defendant has done little to provide Plaintiff and the Class Members with relief for the damages they suffered.

A. Plaintiff Brandon Strong

76. Plaintiff Brandon Strong is an adult individual and a natural person of Montana, residing in Gallatin County, where he intends to stay.

77. WebTPA obtained Plaintiff's information through Plaintiff's former employer on or about July 2023.

78. Plaintiff received a notice letter ("Notice of Data Breach") from Defendant WebTPA dated May 8, 2023 informing him of the Data Breach and the exposure of his Private Information.

79. The notice letter informed Plaintiff that his name, contact information, date of birth, and Social Security number were potentially compromised in the Data Breach.

80. Plaintiff is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him Plaintiff uses two-factor or multifactor authentication to add an extra layer of security to his Private Information.

81. Plaintiff only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

82. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

83. Plaintiff has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later been placed for sale on the dark web.

84. Furthermore, Plaintiff has experienced spam contact as a result of the Data Breach.

85. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

86. As a result of the actual harm he has suffered and the increased imminent risk of future harm from the Data Breach, Plaintiff has spent approximately over one (1) hour combing through his financial records, billing statements, and credit history to stay vigilant against potential fraud or identity theft.

87. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend several hours dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach letter, researching the events surrounding the Data Breach, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

88. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety. Plaintiff has a continuing interest in ensuring that Plaintiff's Private

Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Class Face Significant Risk of Present and Continuing Identity Theft

89. Plaintiff and Class Members suffered injury from the misuse of their PII and PHI that can be directly traced to Defendant.

90. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII and PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

91. In 2021, 32% of persons age 16 or older who received breach notification were victims of multiple types of identity theft.¹⁹

92. As a result of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and Class Members suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their PII and PHI is used;
- b. The diminution in value of their PII and PHI;
- c. The compromise and continuing publication of their PII and PHI;

¹⁹ Erika Harrell, PhD, *Data Breach Notifications and Identity Theft, 2021*, U.S. Bureau of Justice Statistics (Jan. 2024), <https://bjs.ojp.gov/data-breach-notifications-and-identity-theft-2021>.

- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen PII and PHI; and
- h. The continued risk to their PII and PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII and PHI in their possession.

93. Stolen PII and PHI is one of the most valuable commodities on the criminal information black market. According to Prey, a company that develops device tracking and recovery software, stolen PII and PHI can be worth up to \$2,000.00 depending on the type of information obtained.²⁰

94. The value of Plaintiff's and the Class's Private Information on the black market is considerable. Stolen PII and PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

²⁰ Juan Hernandez, *The Lifecycle of Stolen Credentials on the Dark Web*, Prey (Feb. 26, 2024), <https://preyproject.com/blog/lifecycle-stolen-credentials-dark-web>.

95. It can take victims years to spot or identify PII and PHI theft, giving criminals plenty of time to milk that information for cash.

96. One such example of criminals using PII and PHI for profit is the development of “Fullz” packages.²¹

97. Cyber-criminals can cross-reference two sources of PII and PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as “Fullz” packages.

98. The development of “Fullz” packages means that stolen PII and PHI from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class’s phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII and PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to

²¹ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz”, which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. See, e.g., Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SEC. (Sep. 18, 2014), <https://krebsonsecurity.com/tag/fullz/>.

find that Plaintiff's and other members of the proposed Class's stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

99. According to the FBI's Internet Crime Complaint Center (IC3) 2023 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than \$12.5 billion in losses to individuals and business victims.²²

100. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

101. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII and PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

102. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."²³

²² 2023 Internet Crime Report, Fed. Bureau of Investig. (2023), https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf (last accessed Apr. 11, 2024).

²³ *Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMMISSION (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

103. The FTC has issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.²⁴ According to the FTC, data security requires: (1) controlling access to data sensibly; (2) requiring secure passwords and authentication; (3) storing sensitive information securely and protecting it during transmission; (4) segmenting networks and monitoring who is trying to get in and out; (5) securing remote access to networks; (6) applying sound security practices when developing new products; (7) ensuring that third-party service providers implement reasonable security measures; (8) putting in place procedures to keep security current and address potential vulnerabilities; and (9) securing paper, physical media, and devices.²⁵

104. According to the FTC, unauthorized PII and PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.²⁶ The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act (the "FTCA").

105. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ

²⁴Start With Security, A Guide for Business, Fed. Trade Comm'n (Aug. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf.

²⁵*Id.*

²⁶ See *Taking Charge, What to Do If Your Identity is Stolen*, FED. TRADE COMM'N, at 3 (2012), <https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen>.

sufficient measures to detect unauthorized access.”); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) (“[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]” “did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]” and “failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . .”); *In the matter of Dave & Buster’s Inc.*, No. C-4291 (May 20, 2010) (“[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization” and “failed to use readily available security measures to limit access between instore networks . . .”). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. Defendant thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of PII and PHI.

106. Healthcare organizations have become a main target for cybercriminals because they “hold a massive amount of patient data — including medical records, financial information, Social Security numbers, names and addresses. They’re also among the few businesses that stay open 24/7, meaning they might be more likely to prioritize avoiding disruptions and, therefore, more likely to pay a hacker’s ransom.”²⁷

107. Charged with handling highly sensitive PII and PHI including healthcare information, financial information, and insurance information, Defendant knew or should have known the importance of safeguarding the PII and PHI that was entrusted to it. Defendant also knew or should have known of the foreseeable consequences if its data security systems were

²⁷ Elise Takahama, *Why health care has become a top target for cybercriminals*, The Seattle Times (Feb. 25, 2024), <https://www.seattletimes.com/seattle-news/health/why-health-care-has-become-a-top-target-for-cybercriminals/>.

breached. Defendant nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

108. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII and PHI of Plaintiff and over 2.4 million members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

CLASS ACTION ALLEGATIONS

109. Plaintiff brings this class action individually on behalf of himself and on behalf of all members of the following Classes of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. Plaintiff seeks certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3) of the following Nationwide Class (the "Class"):

Nationwide Class

All persons residing in the United States whose Private Information was impacted by the Data Breach—including all persons that Defendant sent a Notice of the Data Breach to (the "Class").

110. The Class defined above is readily ascertainable from information in Defendant's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

111. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or their parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have

been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

112. Plaintiff reserves the right to amend or modify the Class definitions as this case progresses.

113. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

114. **Numerosity.** Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of the approximately 2.4 million individuals whose PII and PHI were compromised by Defendant's Data Breach.

115. **Commonality.** There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

- a. If Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII and PHI;
- b. If Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. If Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

- d. If Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. If Defendant owed a duty to Class Members to safeguard their PII and PHI;
- f. If Defendant breached its duty to Class Members to safeguard their PII and PHI;
- g. If Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- h. If Defendant should have discovered the Data Breach earlier;
- i. If Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;
- j. If Defendant's delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;
- k. If Defendant's method of informing Plaintiff and Class Members of the Data Breach was unreasonable;
- l. If Defendant's conduct was negligent;
- m. If Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;
- n. If Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- o. If Defendant breached implied contracts with Plaintiff and Class Members;
- p. If Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

- q. If Defendant failed to provide notice of the Data Breach in a timely manner, and;
- r. If Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

116. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach. Moreover, Plaintiff and Class Members were subjected to Defendant's uniformly illegal and impermissible conduct.

117. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's counsel are competent and experienced in litigating complex class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Class.

118. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and Class Members' data was stored on the same computer system and unlawfully exposed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

119. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual

Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

120. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

121. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

122. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above.

123. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CLAIMS FOR RELIEF

I. FIRST CAUSE OF ACTION

Negligence

(On Behalf of Plaintiff and the Nationwide Class)

124. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 123 of the Complaint as if fully set forth herein.

125. WebTPA required Plaintiff and Class Members to provide Defendant with Private Information in order to receive Defendant's products and services.

126. By collecting and storing this data in their computer system and network, and sharing it and using it for commercial gain, WebTPA owed a duty of care to use reasonable means to secure and safeguard their computer system—and Plaintiff's and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes so they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

127. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant holds vast amounts of PII and PHI, it was inevitable that unauthorized individuals would at some point try to access Defendant's databases of PII and PHI.

128. After all, Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII and PHI of Plaintiff and Class Members. Thus, Defendant knew, or should have known, the importance of exercising reasonable care in handling the PII and PHI entrusted to them.

129. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII and PHI.

130. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and Class Members, which is

recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

131. Defendant failed to take appropriate measures to protect the PII and PHI of Plaintiff and the Class. Defendant is morally culpable, given the prominence of security breaches in the healthcare industry. Any purported safeguards that Defendant had in place were wholly inadequate.

132. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII and PHI by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches in the healthcare industry, and allowing unauthorized access to Plaintiff's and the other Class Members' PII and PHI.

133. The failure of Defendant to comply with industry and federal regulations evinces Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII and PHI.

134. But for Defendant's wrongful and negligent breach of their duties to Plaintiff and the Class, Private Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII and PHI of Plaintiff and the Class and all resulting damages.

135. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII and PHI. Defendant knew or should have known that

their systems and technologies for processing and securing the PII and PHI of Plaintiff and the Class had security vulnerabilities.

136. As a result of this misconduct by Defendant, the PII, PHI, and other sensitive information of Plaintiff and the Classes was compromised, placing them at a greater risk of identity theft and their PII and PHI being disclosed to third parties without the consent of Plaintiff and the Class.

137. As a direct and proximate result of WebTPA's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in WebTPA's possession and is subject to further unauthorized disclosures so long as WebTPA fails to undertake appropriate and adequate measures to protect the Private Information; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by WebTPA's data breach; (x) the value of the unauthorized access to their PII/PHI permitted by Defendant; and (xi) any nominal damages that may be awarded.

138. As a direct and proximate result of WebTPA's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not

limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses including nominal damages.

139. WebTPA's negligent conduct is ongoing, in that it still possesses Plaintiff's and Class Members' Private Information in an unsafe and insecure manner.

140. Plaintiff and Class Members are entitled to injunctive relief requiring WebTPA to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

II. SECOND CAUSE OF ACTION
Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class)

141. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 123 of the Complaint as if fully set forth herein.

142. WebTPA had had duties arising under HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and the FTC Act to protect Plaintiff's and Class Members' Private Information.

143. WebTPA breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by WebTPA include, but are not limited to, the following: (i) failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information; (ii) failing to adequately monitor the security of its networks and systems; (iii) allowing unauthorized access to Class Members' Private Information; (iv) failing to detect in a timely manner that Class Members' Private Information had been compromised; (v) failing to remove Private Information it was no longer required to retain pursuant to regulations; and (vi) failing to timely and adequately

notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

144. WebTPA's violation of HIPAA, HITECH, and Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

145. Plaintiff and Class Members are consumers within the class of persons that HIPAA, HITECH, and Section 5 of the FTC Act were intended to protect.

146. The harm that has occurred is the type of harm HIPAA, HITECH, and the FTC Act were intended to guard against.

147. The FTC has pursued enforcement actions against businesses and healthcare entities that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

148. WebTPA breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

149. Plaintiff and Class Members were foreseeable victims of WebTPA's violations of HIPAA, HITECH, and the FTC Act. WebTPA knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiff's and Class Members' Private Information would cause damage to Plaintiff and the Class.

150. As a direct and proximate result of WebTPA's negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam

calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in WebTPA's possession and is subject to further unauthorized disclosures so long as WebTPA fails to undertake appropriate and adequate measures to protect the Private Information.

151. As a direct and proximate result of WebTPA's negligence *per se* Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

152. Finally, as a direct and proximate result of WebTPA's negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in WebTPA's possession and is subject to further unauthorized disclosures so long as WebTPA fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

III. THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

153. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 123 of the Complaint as if fully set forth herein.

154. Plaintiff and Class Members conferred a benefit on Defendant by entrusting their Private Information to WebTPA from which WebTPA derived profits.

155. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant

instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide adequate security.

156. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

157. Defendant acquired the PII and PHI through inequitable means in that Defendant failed to disclose the inadequate security practices, previously alleged, and failed to maintain adequate data security.

158. If Plaintiff and Class Members knew that Defendant had not secured their PII and PHI, they would not have agreed to disclose their data to Defendant.

159. Plaintiff and Class Members have no adequate remedy at law.

160. As a direct and direct an proximate result of WebTPA's conduct, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in WebTPA's possession and is subject to further unauthorized disclosures or further entrustment to inadequate third party vendors so long as

WebTPA fails to undertake appropriate and adequate measures to protect the Private Information; (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by WebTPA's data breach; (x) the value of the unauthorized access to their PII/PHI permitted by Defendant; and (xi) any nominal damages that may be awarded.

161. Plaintiff and Class Members are entitled to restitution and/or damages from WebTPA and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by WebTPA from its wrongful conduct, as well as return of their sensitive Private Information and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

162. Plaintiff and Class Members may not have an adequate remedy at law against WebTPA, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

IV. FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Nationwide Class)

163. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 123 of the Complaint as if fully set forth herein.

164. A relationship existed between Plaintiff, the Class Members, and Defendant, which arose from Defendant's acceptance of Plaintiff's and the Class Members' PII and PHI and Defendant's representations of its commitment to protect said PII and PHI.

165. WebTPA became the guardian of Plaintiff's and Class Members' Private Information. WebTPA became a fiduciary, created by its undertaking and guardianship of Plaintiff's and Class Members' Private Information, to act primarily for their benefit. This duty included the obligation to safeguard Plaintiff's and Class Members' Private Information and to timely detect and notify Plaintiff and Class Members in the event of a data breach.

166. The interests of public policy mandates that a fiduciary duty is imputed given Defendant's acceptance of Plaintiff's and the Class Members' Private Information and Defendant's representations of its commitment to protect said Private Information.

167. Defendant breached the fiduciary duty that it owed to Plaintiff and Class Members because Defendant failed to act with the utmost good faith, fairness, honesty, the highest degree of loyalty, ultimately failed to protect the Private Information of Plaintiff and Class Members.

168. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiff and Class Members.

169. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and Class Members would not have occurred.

170. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and Class Members.

171. As a direct and proximate result WebTPA's breaches of its fiduciary duties, Plaintiff and Class Members have suffered or will suffer concrete injury, including, but not limited to: (a) actual identity theft; (b) the loss of the opportunity to determine how and when their Private Information is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft

and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in WebTPA's possession and is subject to further unauthorized disclosures so long as WebTPA fails to undertake appropriate and adequate measures to protect Private Information in its continued possession and ensure that it retains vendors who adequately protect Private Information; (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, and repair the impact of the Private Information compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (h) nominal damages.

172. As a direct and proximate result of WebTPA breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

V. FIFTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

173. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 123 of the Complaint as if fully set forth herein.

174. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into contracts for the provision of administrative services, as well as implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

175. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when they first applied for or obtained administrative services from WebTPA.

176. The valid and enforceable implied contracts to provide administrative services that Plaintiff and Class Members entered into with Defendant and/or its customers include the promise to protect non-public Private Information given to Defendant or that Defendant creates on its own from disclosure.

177. When Plaintiff and Class Members provided their Private Information to Defendant and/or its customers in exchange for administrative services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

178. Defendant and/or its agents solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

179. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

180. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

181. Under the implied contracts, Defendant and/or its customers promised and were obligated to: (a) provide administrative services to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' PII/PHI: provided to obtain such administrative services; and/or created as a result of providing such services. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

182. Both the provision of administrative services and the protection of Plaintiff's and Class Members' Private Information were material aspects of these implied contracts.

183. The implied contracts for the provision of administrative services— contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's privacy policies.

184. Defendant's express representation memorialize and embody the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

185. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To Plaintiff and Class Members, administrative services that do not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than administrative services that adhere to industry-standard data security. Plaintiff and Class Members would not have entrusted their Private Information to Defendant and/or its customers and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

186. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendant and/or its Agents, and paid for the provided services in exchange for, amongst other things, both the provision of administrative services and the protection of their Private Information.

187. Plaintiff and Class Members performed their obligations under the contract when they paid for their administrative services and provided their Private Information.

188. Defendant materially breached its contractual obligation to protect the non-public Private Information Defendant gathered when the sensitive information was accessed by unauthorized personnel as part of the Data Breach.

189. Defendant materially breached the terms of the implied contracts. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiff and approximately 2.4 million Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiff's and the Class Members' Private Information, as set forth above.

190. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

191. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received administrative services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the administrative services with data security protection they paid for and the services they received.

192. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased administrative services from Defendant and/or its affiliated healthcare providers.

193. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

194. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

195. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit and identity monitoring to all Class Members.

VI. SIXTH CAUSE OF ACTION
Declaratory Judgment/Injunctive Relief
(On Behalf of Plaintiff and the Nationwide Class)

196. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 123 of the Complaint as if fully set forth herein.

197. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

198. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' Private Information and whether WebTPA is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Private Information. Plaintiff alleges that WebTPA's data security measures

remain inadequate.

199. WebTPA's April 2023 cybersecurity incident demonstrates the need for injunctive relief for Plaintiff and Class Members. WebTPA has not implemented measures to protect Private Information, leaving Plaintiff and Class Members without a way of protecting themselves.

200. Plaintiff and Class Members continue to suffer injuries as result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

201. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: (a) WebTPA owes a legal duty to secure Plaintiff's and Class Members' Private Information, and to timely notify impacted individuals of a data breach under the common law, Section 5 of the FTC Act, HIPAA, and various state statutes, and (b) WebTPA continues to breach this legal duty by failing to employ reasonable measures to secure Private Information in its possession.

a. Order WebTPA to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with WebTPA's explicit or implicit contractual obligations and duties of care, WebTPA must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. prohibiting WebTPA from engaging in the wrongful and unlawful acts alleged herein;

ii. requiring WebTPA to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

- iii. requiring WebTPA to delete and purge the Private Information of Plaintiff and Class Members unless WebTPA can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- iv. requiring WebTPA to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Private Information;
- v. requiring WebTPA to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on WebTPA's systems on a periodic basis;
- vi. prohibiting WebTPA from maintaining Plaintiff's and Class Members' Private Information on a cloud-based database until proper safeguards and processes are implemented;
- vii. requiring WebTPA to segment data by creating firewalls and access controls so that, if one area of WebTPA's network is compromised, hackers cannot gain access to other portions of WebTPA's systems;
- viii. requiring WebTPA to conduct regular database scanning and securing checks;
- ix. requiring WebTPA to monitor ingress and egress of all network traffic;
- x. requiring WebTPA to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the

employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiff and Class Members;

xi. requiring WebTPA to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with WebTPA's policies, programs, and systems for protecting personal identifying information;

xii. requiring WebTPA to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor WebTPA's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring WebTPA to meaningfully educate all Class Members about the threats that it faces because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

202. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at, or implicating, WebTPA. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

203. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to WebTPA if an injunction is issued. Plaintiff and Class Members will likely be

subjected to substantial identity theft and other damage. On the other hand, the cost to WebTPA of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and WebTPA has a pre-existing legal obligation to employ such measures.

204. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at WebTPA, thus eliminating the additional injuries that would result to Plaintiff and Class Members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, on behalf of himself and all others similarly situated, request the following relief:

- A. An Order certifying this action as a class action and appointing Plaintiff as the Class Representative;
- B. A mandatory injunction directing Defendant to adequately safeguard the PII and PHI of Plaintiff and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete and purge the PII and PHI of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII and PHI;
- v. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;
- vi. prohibiting Defendant from maintaining Plaintiff's and Class Members' PII and PHI on a cloud-based database until proper safeguards and processes are implemented;
- vii. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- viii. requiring Defendant to conduct regular database scanning and securing checks;
- ix. requiring Defendant to monitor ingress and egress of all network traffic;
- x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII and PHI, as well as protecting the PII and PHI of Plaintiff and Class Members;
- xi. requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing

employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring Defendant to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that Defendant provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII and PHI to unauthorized persons;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII and PHI;

E. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiff and the Class leave to amend this Complaint to conform to the evidence produced at trial;

- I. For all other Orders, findings, and determinations identified and sought in this Complaint; and
- J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury for any and all issues in this action so triable as of right.

Dated: May 31, 2024

Respectfully Submitted,

/s/ Bruce W. Steckler
Bruce W. Steckler
Texas Bar I.D. 00785039
STECKLER WAYNE & LOVE PLLC
12720 Hillcrest Road, Suite 1045
Dallas, TX 75230
Telephone: (972) 387-4040
Facsimile: (972) 387-4041
bruce@swclaw.com

Jean S. Martin*
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jeanmartin@ForThePeople.com

Counsel for Plaintiff and the Class

**pro hac vice to be filed*